Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Mathy
Last Name: Vanhoef
Mailing Address: Celestijnenlaan 200A - bus 2402
City: Vlaams-Brabant
Country: Belgium
State or Province: Heverlee
ZIP/Postal Code: 3001
Email Address: vanhoefm@gmail.com
Organization Name:
Comment: See attached file(s).

The attached files may already have been submitted. It was unclear whether the first submission was successful. My apologies for this inconvenience.

See attached file(s).

The attached files may already have been submitted. It was unclear whether the first submission was successful. My apologies for this inconvenience.

A Case For Open Radio Software

Mathy Vanhoef

iMinds-DistriNet, KU Leuven, Belgium
Mathy.Vanhoef@cs.kuleuven.be

Abstract. Recently the Federal Communications Commission (FCC) proposed a rule mandating software security for all radios that are controllable through software. While the motivation behind the rule is understandable, it is argued that the proposed rule is too strict. First, it is argued that the FCC does not have to authority to exercise control over the full software package, but only over the parts directly influencing reception or transmission of signals. Second, the proposed rule makes it impossible to carry out certain research relating to wireless communications. With this in mind, a better device security rule is proposed.

1 Introduction

Due to the explosion of mobile devices, Wi-Fi is more popular than ever. While there are concerns that the available spectrum is becoming overcrowded, the growing bandwidth needs can be met by increasing use of the 5 GHz band. Indeed, recently the Federal Communications Commission (FCC) even widened the available spectrum in the 5 GHz band [14]. Unfortunately, improper usage of the 5 GHz band can cause interference with other systems. These interference issues made the FCC create the *already adpoted* rule that devices operating in the 5 GHz band must prevent third parties from operating the device outside ranges it was certified for [14]. One option to assure this, is to modify the device so it will only run authorized software. Possibly inspired by this rule, the FCC has now proposed a new rule that *all* radio devices should only run authorized software [15]. While this article acknowledges the need for (new) rules to limit intentional interference, it argues that the proposed measures are too strict, and would significantly limit future research into wireless communications.

Arguably the most worrisome downside of the 5 GHz band is possible interference with Terminal Doppler Weather Radar systems. These radar systems are commonly used by airports to detect hazardous weather conditions, and operate in the 5 GHz band. Interference to these systems is deemed unacceptable and potentially life threatening. Unfortunately, the FCC had to deal with numerous cases of intentional interference with radars [12,13,11]. For example, when the weather radar serving Denver International Airport encountered interference, it was found that a device operated by Directlink was responsible for this interference [12]. The device in question was certified to operate within a frequency range of 5745 MHz to 5825 MHz. However, Directlink was operating it on frequency 5630 MHz. In another example, the weather radar serving Salt Lake

City International Airport suffered from interference [13]. Using direction-finding techniques it was found that two devices owned by Utah Broadband were the source of this interference. Both were XtremeRange5 devices, one device operating on frequency 5580, and the other on 5640 MHz. However, the XtremeRange5 is only certified to operate within a frequency range of 5745 MHz to 5825 MHz. Additionally, the Dynamic Frequency Selection (DFS) functionality was purposely disabled by Utah Broadband on both devices. Normally DFS is used to detect the presence of nearby radar systems, and prevent interference in case a radar signal has been detected. In a similar case, Skybeam Acquisition Corporation was using a device outside the frequency range it was certified for, and also intentionally disabled the DFS functionality [11]. This caused interference with the weather radar of Denver International Airport.

These cases illustrate that a device should not be able to operate on frequencies it was not certified for, and that it should not be possible to disable interference-avoidance technologies such as DFS. Since these days most radios are configurable by software, this means there must be safeguards preventing (unauthorized) software from changing the RF parameters outside ranges the device was certified for.

2 Existing Security Rules for U-NII Devices

To reduce interference with weather radars in the 5 GHz band, the FCC adopted new rules to prevent devices from transmitting using unauthorized transmissions powers or frequencies. More specifically, in March 2014 they revised the rules of devices operating in the Unlicensed National Information Infrastructure (U-NII) band [14]. Simplified, the U-NII band corresponds to the 5 GHz frequency band as currently used by Wi-Fi devices. The FCC now mandates that all devices capable of operating in the U-NII band have to be secured so third parties cannot operate the device outside ranges it was certified for. Devices wishing to be certified by the FCC must prove that unauthorized modifications, which could help violate this rule, cannot be made[1]:

> Applications for certification of U-NII devices in the 5.15-5.35 GHz and the 5.47-5.85 GHz bands must include a high level operational description of the security procedures that control the radio frequency operating parameters and ensure that unauthorized modifications cannot be made.

A subsequent section specifies exactly which unauthorized modifications have to be prevented (emphasis mine)[2]:

> 1. Manufacturers must implement security features in any digitally modulated devices capable of operating in any of the U-NII bands, so that *third parties are not able to reprogram the device to operate outside the parameters for which the device was certified.* The

[1] See 47 C.F.R. §2.1033(b)(13)
[2] See 47 C.F.R. §15.407(i) Device Security

software must prevent the user from operating the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved for the device. Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, *electronic signatures in software* or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements and must describe the methods in their application for equipment authorization.

2. Manufacturers must take steps to ensure that DFS functionality cannot be disabled by the operator of the U-NII device.

Note that this rule does not mandate that the software must be digitally signed. It is only one example of techniques that can be used to enforce the rule, manufacturers can still explore other options to assure the device cannot be used outside ranges it was certified for. In other words, while it give examples of which security measures can be used, it does not mandate one specific technique.

One year after introducing the rule, a guideline document was released that provides guidance on the information that should be submitted to the equipment authorization application [16]. In its introduction it is stated that:

> An applicant must describe the overall security measures and systems that ensure that:
>
> 1. Only properly authenticated software is loaded and operating the device.
> 2. The device is not easily modified to operate with RF parameters outside of the authorization.

Surprisingly, the first point is more restrictive than the actual rules! As mentioned, the rules state that a device requires security features to assure it is never operating outside the parameters for which the devices was certified. Software controls are only mentioned as one possible method to assure this. Hence the rules do not require that all software loaded on the device must be authenticated. This incorrect interpretation of the rules is worrisome. Only point two matches the actual rules that must be followed.

The guideline document continues with a series of questions for the manufacturer to demonstrate that the device meets the new security requirements. One of these questions is:

> What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from "flashing" and the installation of third-party firmware such as DD-WRT.

Explicitly mentioning it should not be possible to load DD-WRT is very surprising, as there is no FCC rule requiring such extreme control of all software. Indeed, the actual rules do not prevent loading custom OS software such as

DD-WRT. Manufacturers must only implement security features so the device always operates within radio parameters for which the device was certified. This does not inherently require that all software must be signed and approved. Unsurprisingly, this guideline question (as well as newly proposed rules) caused enormous response and concern in the public [25]. Fortunately, guidelines document do not constitute rules, hence manufacturers are not obliged to follow these guidelines. As stated in [10]:

> [..] the staff guidance provided in the following KDB publications is intended to assist the public in following Commission requirements and does not constitute rules. Accordingly, the guidance is not binding on the Commission and will not prevent the Commission from making a different decision in any matter that comes to its attention for resolution. The guidance publications [..] do not necessarily represent the only acceptable methods for demonstrating compliance.

Hence manufacturers are not required to prevent things such as flashing. Nevertheless, this incorrect interpretation of the rules is very worrisome. It's not difficult to imagine that some manufacturers will follow the guidelines just to be on the safe side, to assure their device will be certified. Rules or guidelines should not motivate manufacturers to digitally sign and protect *all* software. This would leave users with little freedom. Hence it is better to remove the flashing question from the guideline, and also to remove the line saying that only authenticated software can be loaded on the device. It may even be good to state the opposite! Namely, that it's perfectly fine to allow flashing of any operating system on the router, as long as the radio always remains sufficiently secured (see Section 5).

3 Proposal of Software Security for all Radio Devices

In July 2015 the FCC proposed that practically *all* radio devices should only run authorized software [15], not just those operating in the 5 GHz U-NII band. Unlike the security rules for U-NII devices, these rules explicitly mention that only approved software can be loaded on the device. Manufacturers cannot explore alternative methods to assure the device only operates within parameters it was certified for. The rule change is mainly motivated by the observation that nowadays most radio devices use software to control RF parameters (frequency, transmit power, etc), and that by software changes alone it can be possible to operate the device on unauthorized RF parameters.

In the proposed rule change, first the definition of a Software Defined Radio (SDR) is updated to [15, §2.1]:

> A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.

Previously a device only had to be treated as an SDR if the software was explicitly designed or expected to be modified by a party other than the manufacturer. But with this change, any device with software control over RF parameters has to be treated as an SDR, even if it's not expected to be used as a traditional SDR. What are the special requirements surrounding an SDR? Software security safeguards to assure compliance with the rules (emphasis mine) [15, §2.1042(e)]:

> Manufacturers of any radio including certified modular transmitters which includes a software defined radio must take steps to ensure that *only software that has been approved with a particular radio can be loaded into that radio.* The software must not allow the installers or end-user to operate the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved. Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements.

Not that this SDR rule explicitly states that the device must only run authorized software. In contrast, the U-NII device security rule limited itself only to radio operations: it only mandates that third parties cannot operate the radio outside ranges it was certified for. Related to this, in Section 4 it is argued that the FCC does not have authority over the complete software package. The FCC only has authority over the parts influencing radio operations, and hence the proposed SDR rule it outside the FCC's authority.

A description of how the SDR rule is met must be provided during the equipment authorization process [15, §2.1033(a)(4)(i)]:

> [..] the description must include details of the equipments capabilities for software modification and upgradeability, including all frequency bands, power levels, modulation types, or other modes of operation for which the device is designed to operate, whether or not the device will be initially marketed with all modes enabled. The description must state which parties will be authorized to make software changes (e.g., the grantee, wireless service providers, other authorized parties) and the software controls that are provided to prevent unauthorized parties from enabling different modes of operation. Manufacturers must describe the methods used in the device to secure the software in their application for equipment authorization [..]. The applicant must provide an attestation that only permissible modes of operation may be selected by a user.

This means there are now two rules regarding device security. There is the (existing) rule for U-NII devices, and the proposed rule for SDRs. Strangely, since most U-NII devices will have to be classified as SDRs under the newly proposed rules, this means they must adhere to both security rules. It is be better to combine and simplify these two cases (see Section 5).

The rules commonly mention the terms device and radio. Unfortunately, these terms are not given precise definitions. This makes it difficult to anticipate the impact of statements such as "only approved software can be loaded on the device". Does this mean the complete operating system needs to be secure? Or only the driver? Or just the firmware that is loaded into the radio component? Ideally this should not matter. If the rules are restricted to only cover and protect operations directly influencing radio parameters, and not the complete software package, the precise definition of these terms becomes less important. For example, since it is generally the firmware that directly controls radio parameters, the operating system (including drivers) would no longer have to be protected.

4 No Authority Over Complete Software Package

Nowadays, the firmware (software) of a radio component of a device performs more tasks than merely controlling RF parameters. Generally it also contains code to process incoming and outgoing frames, with as main goal to offload common tasks from the main host. Examples include calculating and verifying checksums, fragmenting and aggregating frames, detecting retransmitted frames as duplicates, dropping packets destined for other devices, etc. As a more specialized example, software for Wi-Fi radios are commonly also capable of collecting nearby SSIDs autonomously. The resulting list of SSIDs can then be requested by the host computer. All these operations are programmed in the same software which also controls RF parameters (for more examples see Section 6). It seems unreasonable for the FCC to exercise authority over these non-RF operations by requiring that these operation can only be performed by approved software. In other words, the FCC does not have the authority to mandate that the *complete* software package must be secured. They only have authority over parts controlling RF-parameters and parts that directly influence reception and transmission of signals.

This position is consistent with the decision made in American Library Association v. FCC [1]. The case dealt with the broadcast flag, a technology to prevent unauthorized copying and redistribution of digital media (emphasis mine):

> The broadcast flag [..] is a digital code embedded in a digital broadcasting stream, which prevents digital television reception equipment from redistributing digital broadcast content. The effectiveness of the broadcast flag regime is dependent on programming being flagged and on devices capable of receiving broadcast DTV signals (collectively "demodulator products") being able to recognize and give effect to the flag. Under the rule, new demodulator products (e.g., televisions, computers, etc.) must include flag recognition technology. This technology, in combination with broadcasters' use of the flag, would prevent redistribution of broadcast programming. *The broadcast flag does not have any impact on a DTV broadcast transmission.* The flags only effect is to limit the capacity of receiver apparatus to redistribute broadcast content after a broadcast transmission is complete.

Essentially the broadcast flag rule required manufacturers to implement software assuring the flag was always respected. However, it was noted that this flag did not have an impact on reception or transmission itself. This fact proved essential in the final ruling (emphasis mine) [1]:

> [..] the agencys general jurisdictional grant does not encompass the regulation of consumer electronics products that can be used for receipt of wire or radio communication *when those devices are not engaged in the process of radio or wire transmission.*

Clearly most of the Operating System, including userland programs, are not used for receipt or transmission of radio communications. Hence the FCC does not have the authority to prevent flashing software such as DD-WRT (see Section 2). Moreover, since a large part of the software running on modern radio devices also does not directly impact radio or wire transmission, the FCC also does not have authority over the *complete* software running on these devices.

In analogy with the ALA vs. FCC ruling, it is unreasonable for the FCC to have the power to regulate all software loaded on a radio device. They cannot require that the full software package should be protected by security mechanisms. Indeed, the final ruling in the broadcast flag case states (emphasis mine) [1]:

> In this case, all relevant materials concerning the FCCs jurisdiction—including the words of the Communications Act of 1934, its legislative history, subsequent legislation, relevant case law, and Commission practice—confirm that *the FCC has no authority to regulate consumer electronic devices that can be used for receipt of wire or radio communication when those devices are not engaged in the process of radio or wire transmission.*

Effectively the FCC is proposing rules (only allowing authorized software) over functionality it does not have authority over (operations not involving receipt or transmission of radio or wire communication). Note that accepting the currently proposed rule would directly harm certain users. Namely, researchers relying on modified Broadcom firmware that forwards all *already decoded frames* to the host [20], would no longer be able to apply these modifications. The changes to the firmware in way no impacts RF-parameters, transmission, or reception. Put differently, the modified operations take place after any form of reception or transmission have occurred. Hence the FCC does not have authority to forbid these modifications. The broadcast flag case confirms this [1]:

> In sum, we hold that, at most, the Commission only has general authority under Title I to regulate apparatus used for the receipt of radio or wire communication while those apparatus are engaged in communication.

Hence the proposed SDR software security rules lie outside the authority of the FCC. Nevertheless, the need to prevent devices from operating in an unauthorized manner remains. Hence a modified rule, which addresses the problems above, is proposed in the next section.

5 Proposed Modification to Software Security Rule

With the previous discussions in mind, a better replacement of the proposed SDR software security rule [15, §2.1042(e)] is the following:

> Manufacturers of any radio including certified modular transmitters which includes a software defined radio must implement security features so that third parties are not able to operate the device outside radio parameters (operating frequencies, output power, modulation types or other radio frequencies parameters) for which the device was certified. Manufacturers may use means including, but not limited to, hardware enforced limits on radio parameters when third party software is loaded, electronically signed configuration files which the hardware or radio can decode to verify that the device is authorized to use new radio parameter ranges for which the device was initially not certified.

If this change is adopted, rules regarding the equipment authorization process [15, §2.1033(a)(4)(i)] do not have to be modified. The main idea behind the proposed rule is that a hardware "barrier" limits radio parameters to authorized values only (e.g., the parameters advertised in the initial FCC certification of the device). By supplying a small configuration file that is signed by the manufacturer, it is possible to enable additional radio parameters. For example, a manufacturer can enable new a channel by specifying this in the configuration file, and then signing this file. A few remarks are in place:

1. The proposed rule avoids stating that all software loaded on the device must be secured. Instead, it purposely limits itself only to radio operations. Hence this rule is within authority of the FCC to propose and adopt.
2. Third parties can modify the software, with the assurance that the radio will only operate using authorized radio parameters. In other words, third parties can modify operations which are unrelated to transmission or reception of signals, while only being able to operate the radio in an authorized manner.
3. The (original) manufacturer can include a signed configuration file to, for example, unlock additional channels or transmit powers. Note that this does not require signing the complete software package. Instead, the signature is created only over a small configuration file. If the signature is valid, the radio (hardware) can read the configuration file and unlock the specified radio parameters. Essentially the signature proves the device has been authorized by the FCC and/or manufacturer to operate under new radio parameters. Third parties cannot modify this configuration file since that would invalidate the signature. Hence, while third parties can always modify functionality unrelated to radio operations, they cannot influence allowed radio parameters.

To conclude, third parties cannot create valid signatures, so they can't unlock additional radio parameters themselves. On the other hand, third parties can still include an existing configuration file, signed and issued by the original manufacturer, to unlock new parameters. Hence even modified software can use

the new radio parameters, while still only being able to operate within authorized ranges.

As already mentioned, it is also be worthwhile to consider whether part of the device security rules for U-NII devices can be simplified. Point one of rule 47 C.F.R. §2.1033(b)(13)[3] is no longer needed if the more general software security rules will be accepted. In fact, the proposed SDR rule in this section is based on the security rules for U-NII devices.

6 Research Requiring Open Radio Software

This section describers several research projects where software, responsible for controlling the radio, has been modified to carry out experiments. Locking down the software of radio chips would make this kind of research impossible, or at the very least significantly more expensive. All the examples that will be listed, can be carrier out without operating in unlicensed frequencies, transmit powers, modulations, etc. Put differently, when only securing the control of radio parameters, the research listed below can still be carrier out. The problem with the proposed rules, however, is that it locks down all software.

The first set of examples are works that modify the open source MadWifi driver. Combined with an open source version of the Hardware Abstraction Layer (HAL), this driver gives the user a high level of control received and transmitted Wi-Fi packets. Several researchers modified the MadWifi driver to create, experiment with, and evaluate research prototypes [2]. A few relevant examples are:

Software MAC [28,36,35] A software system that allows researchers to use inexpensive, commodity wireless networking cards to experiment with new (multi-channel) MAC layer protocols.

Overlay MAC [32] A layer on top of the standard 802.11 MAC to mitigate some of its problems. Works only under the assumption that the radio immediately transmits outgoing frames, which is possible with MadWifi.

Opportunistic Retransmission [27] A novel link-layer protocol where overhearing nodes act as relays in case there was a failed transmission. Implementation and evaluation of the protocol was done by modifying MadWifi.

Rate Adaptation [23,29] A rate adaptation algorithm designed for high-latency systems that has been implemented and testing using MadWifi.

Rate Adaptation in Mesh Networks [4] By determining the cause of lost packets (collisions, channel errors, etc.) network throughput can be drastically increased. MadWifi was used to test their algorithm.

Cross-Layer Designs [3] Provides a platform for creating cross-layer designs with 802.11 protocols. Exports link-layer information such as per-station RSSI, number of failed receptions, number of (re)transmitted frames, etc.

[3] This concerns security features so third parties cannot operate the device outside parameters for which the device was certified.

Media Access Control [26] A flexible software platform for developing and evaluating CSMA protocols, created by modifying MadWifi. Offers control over backoff machanisms, retransmission policies, and packet timings.

Adaptive RTS [7] Reduces the overhead of Request-To-Send (RTS) and Clear-to-Send (CTS) protocols by only using in situations where frame loss is likely to occur.

Long Distance Networks [30] Creation of a custom protocol for use in long distance wireless networks. Uses MadWifi with a proprietary Hardware Abstraction Layer (HAL) that is able to turn off carrier sense.

There are many more examples like these, listing them all is out of scope for this article. Open source drivers of newer Atheros devices are also commonly used by researchers, some examples being:

Selfish Behaviour [33] Modified the operation of Atheros chips to implement selfish behaviour in practice, and to subsequently detect and punish it.

Carrier Sense [22] Studies the effectiveness of the carrier sense mechanism. To carry out some experiments they had to modify the operation of Atheros chips to disable carrier sense.

Capture Effect [24] Studies the capture effect in 802.11 networks. During experiments they relied on custom (re)transmit limits, minimum and maximum contention windows sizes, and the ability to disable noise calibration.

Fairness and Capture Effect [17] The capture effect in 802.11 networks reduces throughput fairness among stations. By taking control of transmit power, retransmission limits, contention window adjustments, and AIFS control, it is shown that fairness can be restored, even when the capture effect takes places.

Low-Layer Security [38] Illustrates the impact of several low-layer attacks against the 802.11 protocol, e.g., reactive jamming and channel-based man-in-the-middle attacks. It is then shown these attacks facilitate attack against higher-layer protocols.

Channel Width [8] Determines the influence of channel width on throughput, range, and power consumption. The operation of Atheros devices is modified so it uses channel widths of 5, 10, and 40 GHz.

Interestingly, there is even a project specifically aimed at creating open source firmware. Called the OpenFWWF project, they provide open source firmware for certain Broadcom chips [18]. It was created by first reverse engineering closed source firmware. OpenFWWF has been used in several research works:

Open Source Firmware [18] A project where Broadcom Wi-Fi firmware is reversed, and subsequently an open source variant has been made.

Software MAC [37] Relies on the open source firmware to create a programmable wireless platform that can be used to implement and test custom MAC protocols.

Reactive Jamming [6] Relies on OpenFWWF to implement reactive jamming in 802.11 networks. This is used as a friendly jammer to increase network security.

Deterministic Medium Access Control [34] Implementation of Carrier Sense Multiple Access with Enhanced Collision Avoidance (CSMA/ECA), which guarantees a collision-free schedule under ideal conditions.

Software of other manufacturers has also been modified to carry out research experiments. A few interesting examples are:

Channel State Information [19] Modified firmware of the Intel WiFi Link 5300 wireless NIC so it exports Channel State Information (CSI). These CSI measurements provide a detailed picture of the wireless channel conditions and can be used to select more optimal transmission rates.

Packet Injection [5] Modifies the memory of the iPAQ H3600 at runtime in order to inject arbitrary 802.11 frames.

Monitor Mode [20] Modified firmware of Broadcom radios so it forwards all received frames to the host.

Long-Range Mesh Networks [31] Design of a new MAC protocol for long-distance mesh networks. Requires being able to disable carrier sense and ACK frames, which was possible using Intersil Prism cards.

This kind of research into wireless technologies is vital to meet growing demands. Furthermore, this research can have a direct impact on society. For example, it is thanks to open source mesh software that the Sayada city in Tunisia was able to create their own wireless mesh network [21]. This was done to counter years of government censorship. Their network consists of 12 routers located on rooftops, and gives users access to maps of Tunisia, free books, Wikipedia, chat and file sharing, etc. Without public research into wireless technologies, this likely would not have been possible.

Finally it is important to remark that software for radio devices may also contain vulnerabilities [9]. Normally, if the device is no longer maintained by the original manufacturer, security researchers may provide their own patches that mitigate the vulnerability. If the proposed rule is adopted, this is no longer possible, and users are likely left with insecure devices.

7 Conclusion

The proposed rules by the FCC are too strict. They explicitly mandate that only approved software can run on the radio. Manufacturers are not given the opportunity to explore other means for securing radio operations. Additionally, a strong case can be made that the FCC does not have the authority to exercise control over non-RF operations, that are also present in radio software (e.g. calculating and verifying checksums, aggregating frames, etc). A better approach is to only mandate that the radio must be secured so it only operates using authorized radio parameters (frequency, transmission power, modulation, etc). This gives manufacturers freedom of which security design or technology to employ, and does not force signed or otherwise protected software (as long as the radio will only operate using allowed radio parameters). Moreover, since the modified rule only covers reception or transmission of radio signals, the FCC does have the authority to adopt and enforce this rule.

References

1. American Library Association v. FCC, 406 F.3d 689 (D.C. Cir. 2005).
2. Publicity of MadWifi. Retrieved 13 Aug. 2014, from `http://madwifi-project.org/wiki/Publicity`.
3. H. Aıache, V. Conan, J. Leguay, and M. Levy. Xian: Cross-layer interface for wireless ad hoc networks. *MEDHOCNET 2006*, 2006.
4. E. Ancillotti, R. Bruno, and M. Conti. Experimentation and performance evaluation of rate adaptation algorithms in wireless mesh networks. In *Proceedings of the 5th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, 2008.
5. J. Bellardo and S. Savage. 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. In *Proc. of the 12th USENIX Security Symp.*, 2003.
6. D. S. Berger, F. Gringoli, N. Facchi, I. Martinovic, and J. Schmitt. Gaining insight on friendly jamming in a real-world IEEE 802.11 network. In *WiSec*, 2014.
7. S. Byeon, H. Lee, J. I. Kim, W. S. Cho, and S. Choi. Designing adaptive rts for madwifi-based wlan device. In *Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on*, 2012.
8. R. Chandra, R. Mahajan, T. Moscibroda, R. Raghavendra, and P. Bahl. A case for adapting channel width in wireless networks. In *Proc. of the ACM SIGCOMM 2008 Conf. on Data Comm.*, 2008.
9. Core Security. Advisory: Broadcom DoS on bcm4325 and bcm4329 devices. Retrieved 9 Oct. 2015, from `http://www.coresecurity.com/content/broadcom-input-validation-BCM4325-BCM4329`.
10. Federal Communications Commission (FCC). OET major guidance draft publications. Retrieved 13 Sept. 2015, from `https://apps.fcc.gov/oetcf/kdb/reports/GuidedPublicationList.cfm`.
11. Federal Communications Commission (FCC). Skybeam acquisition corporation, notice of apparent liability for forfeiture and order. 27 FCC Rcd 11337, 2012.
12. Federal Communications Commission (FCC). Directlink, llc, notice of apparent liability for forfeiture and order. 28 FCC Rcd 37, 2013.
13. Federal Communications Commission (FCC). Utah broadband, notice of apparent liability for forfeiture and order. 28 FCC Rcd 11604, 2013.
14. Federal Communications Commission (FCC). Revision of part 15 of the commission's rules to permit unlicensed national information infrastructure (U-NII) devices in the 5 GHz band, first report and order, ET Docket No. 13-49. 29 FCC Rcd 4127, March 2014.
15. Federal Communications Commission (FCC). Amendment of parts 0, 1, 2, 15 and 18 of the commission's rules regarding authorization of radiofrequency equipment, notice of proposed rule making, ET Docket No. 15-170. July 2015.
16. Federal Communications Commission (FCC). Configuration Control: Software security requirements for U-NII devices (594280 d01 v01r02). March 2015.
17. S. Ganu, K. Ramachandran, M. Gruteser, I. Seskar, and J. Deng. Methods for restoring MAC layer fairness in IEEE 802.11 networks with physical layer capture. In *REALMAN*, 2006.
18. F. Gringoli and L. Nava. OpenFWWF: Open firmware for WiFi networks. Retrieved from `http://www.ing.unibs.it/~openfwwf/`.
19. D. Halperin, W. Hu, A. Sheth, and D. Wetherall. Tool release: Gathering 802.11n traces with channel state information. *ACM SIGCOMM CCR*, 2011.
20. O. Ildis, Y. Ofir, and R. Feinstein. Wardriving from your pocket. REcon, 2013.

21. T. O. T. Institute. Case study: Mesh sayada. Retrieved 26 Sept. 2015, from `https://commotionwireless.net/files/posts/041814-Case-Study-Sayada.pdf`, 2014.
22. K. Jamieson, B. Hull, A. Miu, and H. Balakrishnan. Understanding the real-world performance of carrier sense. In *In Proc. of the ACM SIGCOMM Workshop on Experimental Approaches to Wireless Network Design*, 2005.
23. M. Lacage, M. H. Manshaei, and T. Turletti. Ieee 802.11 rate adaptation: a practical approach. In *Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pages 126–134. ACM, 2004.
24. J. Lee, W. Kim, S.-J. Lee, D. Jo, J. Ryu, T. Kwon, and Y. Choi. An experimental study on the capture effect in 802.11a networks. In *Proc. of the 2nd ACM Intl. Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization*, 2007.
25. LibrePlanet. Save wifi: Publicity, news, and blogs. Retrieved 4 Oct. 2015, from `https://libreplanet.org/wiki/Save_WiFi#Publicity.2C_News.2C_and_Blogs`.
26. M.-H. Lu, P. Steenkiste, and T. Chen. Flexmac: a wireless protocol development and evaluation platform based on commodity hardware. In *Workshop on Wireless network testbeds, experimental evaluation and characterization*, 2008.
27. M.-H. Lu, P. Steenkiste, and T. Chen. Opportunistic retransmission in WLANs. *Mobile Computing, IEEE Transactions on*, 11(12), 2012.
28. M. Neufeld, J. Fifield, C. Doerr, A. Sheth, and D. Grunwald. SoftMAC - flexible wireless research platform.
29. S. Pal, S. R. Kundu, K. Basu, and S. K. Das. Ieee 802.11 rate control algorithms: Experimentation and performance evaluation in infrastructure mode. In *Passive and Active Measurement Conference*, 2006.
30. R. K. Patra, S. Nedevschi, S. Surana, A. Sheth, L. Subramanian, and E. A. Brewer. Wildnet: Design and implementation of high performance wifi based long distance networks. In *NSDI*, 2007.
31. B. Raman and K. Chebrolu. Design and evaluation of a new mac protocol for long-distance 802.11 mesh networks. In *Proceedings of the 11th annual international conference on Mobile computing and networking (MobiCom)*, 2005.
32. A. Rao and I. Stoica. An overlay mac layer for 802.11 networks. In *International conference on Mobile systems, applications, and services (MobiSys)*, 2005.
33. M. Raya, J.-P. Hubaux, and I. Aad. DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots. In *MobiSys*, 2004.
34. L. Sanabria-Russo, J. Barcelo, A. Faridi, and B. Bellalta. Wlans throughput improvement with csma/eca. In *Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on*, 2014.
35. A. Sharma and E. M. Belding. Freemac: framework for multi-channel mac development on 802.11 hardware. In *Proceedings of the ACM workshop on Programmable routers for extensible services of tomorrow*, 2008.
36. A. Sharma, M. Tiwari, and H. Zheng. Madmac: Building a reconfiguration radio testbed using commodity 802.11 hardware. In *IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, 2006.
37. I. Tinnirello, G. Bianchi, P. Gallo, D. Garlisi, F. Giuliano, and F. Gringoli. Wireless mac processors: Programming mac protocols on commodity hardware. In *INFOCOM, 2012 Proceedings IEEE*, 2012.
38. M. Vanhoef and F. Piessens. Advanced Wi-Fi attacks using commodity hardware. In *ACSAC*, 2014.

Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, DC 20554

In the Matter of	)	
	)	
Amendment of Part 0, 1, 2, 15 and 18 of the	)	ET Docket No. 15-170
Commission's Rules regarding Authorization	)	
Of Radio frequency Equipment	)	
	)	
Request for the Allowance of Optional	)	RM-11673
Electronic Labeling for Wireless Devices	)	

Comments of Mathy Vanhoef[1]

Mathy Vanhoef
Doctoral Researcher in wireless security
KU Leuven, Dept. Computerwetenschappen[2]
Celestijnenlaan 200a, bus 2404
Heverlee, 3001, Belgium

9 October 2015

---

[1] The paper *A Case For Open Radio Software* gives a more detailed version of these comments, including additional information behind the motivation of these rules, and a larger overview of research projects that would be affected by the proposed rules.

[2] The views and opinions expressed herein are those of the author and do not necessarily reflect the views of KU Leuven, its affiliates, or its employees.

1. Summary

The rules proposed by the Commission, which require device security for all radios that are controllable through software[3], are too strict and broad. By explicitly mandating that only approved software can run on these devices, the Commission is risking to act outside the scope of its delegated authority. As stated in the American Library Association v. FCC case, which dealt with regulations regarding the broadcast flag, the Commission cannot exercise authority over devices when those devices are not in the process of receiving or transmitting signals.[4] Since the software loaded on a radio generally performs more tasks than modulating or demodulating a signal, i.e., it performs several additional tasks after receiving or transmitting a signal, the Commission cannot exercise control over the full software package loaded into a radio. Additionally, the rules proposed by the Commission would harm research into wireless communications. In order to avoid these two pitfalls, a modified and improved device security rule is proposed, which only covers operations that directly influence reception or transmission of signals. The proposed modification is based on existing security rules for devices capable of operating in the U-NII bands.[5] Hence adopting this modification may even simplify the distinction between non U-NII and U-NII devices, as both would be covered by the same rule.

2. Introduction

In response to numerous cases where U-NII devices were intentionally interfering with Terminal Doppler Weather Radar systems,[6] the Commission strengthened the device security rules of U-NII devices.[5] This was understandable, as most interference issues with radars were caused by third parties

---

[3] See *Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment*, Notice of Proposed Rulemaking, ET Docket No. 15-170.

[4] See *American Library Association v. FCC*, 406 F.3d 689 (D.C. Cir. 2005).

[5] See *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, First Report And Order*, ET Docket No. 13-49, 29 FCC Rcd 4127.

[6] For example, see *Skybeam Acquisition Corporation, Notice of Apparent Liability for Forfeiture and Order* (27 FCC Rcd 11337), *Utah Broadband, Notice of Apparent Liability for Forfeiture and Order* (28 FCC Rcd 11604), and *Directlink, LLC, Notice of Apparent Liability for Forfeiture and Order* (28 FCC Rcd 37). A more complete list of examples can be found in ET Docket No. 13-49, 29 FCC Rcd 4127.

operating the device outside radio parameters for which the device was certified. More specifically, the Commission added the following rule (emphasis mine):

> Manufacturers must implement security features in any digitally modulated devices capable of operating in any of the U-NII bands, so that *third parties are not able to reprogram the device to operate outside the parameters for which the device was certified*. The software must prevent the user from operating the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved for the device. *Manufacturers may use means including, but not limited to* the use of a private network that allows only authenticated users to download software, *electronic signatures* in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements and must describe the methods in their application for equipment authorization.

Note that the rule restricts itself only to radio parameters, i.e., to operations or configurations that directly impact the transmission or reception of signals. It does not claim authority over the full software package loaded on the radio. Indeed, only as an example does it list electronic software signatures as a possible method to meet the security rules. Manufacturers are still allowed to explore alternative means to meet this device security rule. For example, if a manufacturer constructs a hardware barrier that assures the radio can only operate using allowed radio parameters, the radio can run third party software without risk of violating this rule.

Recently the Commission released a Notice of Proposed Rulemaking (NPRM) that proposed security rules for any device whose radio operations where controllable through software.[7] This was done by first updating the definition of Software Defined Radios (SDRs) to the following (emphasis mine):

> A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission

---

[7] See *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, First Report And Order*, ET Docket No. 13-49, 29 FCC Rcd 4127.

rules, *can be altered by making a change in software without making any changes to hardware* components that affect the radio frequency emissions.

Previously a device only had to be treated as a Software Defined Radio (SDR) if the software of the device was explicitly designed or expected to be modified by a party other than the manufacturer. With this change, any device having software control over radio parameters or operations has to follow the existing device security rule of SDRs. This existing rule for SDR devices is (emphasis mine):[8]

> Manufacturers of any radio including certified modular transmitters which includes a software defined radio must take steps to *ensure that only software that has been approved with a particular radio can be loaded into that radio*. The software must not allow the installers or end-user to operate the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved. Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements.

While this rule may have been reasonable when it only covered devices that were explicitly designed and expected to be used as SDRs, the updated definition of an SDR drastically changes the impact of this rule. Now all radios that are controllable through software must only run approved software. In contrast, the previously mentioned U-NII device security rule limits itself only to protecting radio operations: it only mandates that third parties cannot operate the radio outside ranges it was certified for, and does not require that only approved software can run on the radio.

Furthermore, it is unclear which parts of the system should only run approved software. Does only the software directly running on the radio (i.e., the firmware) have to be approved? Or do drivers also have to be approved? What about software packages such as DD-WRT? This depends on the precise definition of "radio". However, ideally this definition should not matter. If the rules are modified to only cover and protect operations directly influencing transmission and reception of signals, and avoid requiring that only approved software is allowed, the precise definition of these terms becomes less important. Indeed, such a modification of the rule does not require that only approved software can run

---

[8] See 47 C.F.R. §2.1042(e)

on the radio, since it allows manufacturers to explore alternative methods to assure third parties cannot operate the radio in an unauthorized manner.[9]

3. No Authority Over Full Software Package

Unlike for SDRs, the software loaded into a radio or device that is built for a specific purpose, generally performs more tasks than merely (de)modulating signals or controlling radio parameters. It also contains code to process incoming and outgoing frames, with as main goal to offload common tasks from the main host. Examples include calculating and verifying checksums, fragmenting and aggregating frames, detecting retransmitted frames as duplicates, dropping packets destined for other devices, etc. As a more specialized example, software for Wi-Fi radios are commonly also capable of collecting nearby SSIDs autonomously. All these operations are present in the same software which also controls radio parameters. It seems unreasonable for the Commission to claim authority over these non-RF operations by requiring that these operation can only be performed by approved software. Put differently, by updating the definition of SDRs, the Commission has, perhaps unknowingly, stepped outside its delegated authority, by mandating that the complete software package must be secured.

This standpoint matches the ruling in American Library Association v. FCC.[10] The case dealt with the broadcast flag, a feature to prevent unauthorized copying of digital media (emphasis mine):

> The broadcast flag [..] is a digital code embedded in a digital broadcasting stream, which prevents digital television reception equipment from redistributing digital broadcast content. The effectiveness of the broadcast flag regime is dependent on programming being flagged and on devices capable of receiving broadcast DTV signals (collectively "demodulator products") being able to recognize and give effect to the flag. Under the rule, new demodulator products (e.g., televisions, computers, etc.) must include flag recognition technology. This technology, in combination with broadcasters' use of the flag, would prevent redistribution of broadcast programming. *The broadcast flag does not have any impact on a DTV broadcast transmission.* The flag's only effect is to limit the capacity of receiver apparatus to redistribute broadcast content after a broadcast transmission is complete.

---

[9] See section *Proposed Rule Modification* of this comment.

[10] American *Library Association v. FCC*, 406 F.3d 689 (D.C. Cir. 2005)

Essentially the broadcast flag rule required manufacturers to implement software assuring the flag was always respected. However, it was noted that this flag did not have an impact on reception or transmission itself. This fact proved essential in the final ruling (emphasis mine):

> [..] the agency's general jurisdictional grant does not encompass the regulation of consumer electronics products that can be used for receipt of wire or radio communication *when those devices are not engaged in the process of radio or wire transmission*.

Since a large part of the software running on modern radio devices does not directly impact radio or wire transmission, the Commission does not have authority over the complete software package running on these devices. In analogy to the American Library Association v. FCC ruling, it is unreasonable for the Commission to regulate all software loaded on a radio device (emphasis mine):

> In this case, all relevant materials concerning the FCC's jurisdiction---including the words of the Communications Act of 1934, its legislative history, subsequent legislation, relevant case law, and Commission practice---confirm that *the FCC has no authority to regulate consumer electronic devices that can be used for receipt of wire or radio communication when those devices are not engaged in the process of radio or wire transmission*.

Effectively the Commission has proposed rules (only allowing approved software) over functionality it does not have authority over (operations not involving receipt or transmission of radio or wire communication). As the broadcast flag case states:[11]

> In sum, we hold that, at most, the Commission only has general authority under Title I to regulate apparatus used for the receipt of radio or wire communication while those apparatus are engaged in communication.

Hence the proposed rules lie outside the authority of the Commission.

---

[11] See *American Library Association v. FCC*, 406 F.3d 689 (D.C. Cir. 2005)

4. Research Requiring Open Radio Software

A significant amount of research projects rely on the ability to modify the software running on a radio. Indeed, even the author of this comment has done research where access to the software running on a radio was essential to perform the needed experiments.[12] For an overview and description of other research works requiring such access, we refer to section 6 of the paper "A Case For Open Radio Software".[13] One important example is a project where the proposed device security rules would *directly* harm the project and its users. This project modifies closed source Broadcom Wi-Fi software so it forwards all already demodulated Wi-Fi frames to the host computer.[14] The modified software can then be used by researchers in a mobile phone to easily monitor all nearby Wi-Fi traffic. Such monitor functionality is essential when assessing the security of a network, to investigate network problems, to understand and solve problems in custom implementations of communication schemes (i.e., custom network protocols), and so on. The rules currently proposed by the Commission would no longer allow these modifications, since only approved software can be run on the radio. This directly harms all researchers relying on the modified Broadcom software.

More importantly, the modifications made to the Broadcom software, i.e., software running on the radio device, in no way impact radio operations, transmission, or reception of signals. Put differently, the modified operations take place after reception or transmission have occurred. This means that under the alternative security rule proposed in the next section, these modifications are allowed, while still assuring that third parties cannot operate the radio in an unauthorized manner.

5. Proposed Rule Modification

A modified proposal of the SDR software security rule[15] is the following:

> Manufacturers of any radio including certified modular transmitters which includes a software defined radio must implement security features so that third parties are not able to operate the device outside radio parameters (operating frequencies, output power,

---

[12] M. Vanhoef and F. Piessens. *Advanced Wi-Fi Attacks Using Commodity Hardware*. ACSAC 2014.
[13] *A Case For Open Radio Software*, Mathy Vanhoef, 2015
[14] O. Ildis, Y. Ofir, and R. Feinstein. *Wardriving from your pocket*. REcon, 2013.
[15] See 47 C.F.R. §2.1042(e)

modulation types, or other radio frequencies parameters) for which the device was certified. Manufacturers may use means including, but not limited to, hardware enforced limits on radio parameters when third party software is loaded, electronically signed configuration files which the hardware or radio can decode to verify that the device is authorized to use new radio parameter ranges for which the device was initially not certified.

Note that this rule is similar to the existing rule for U-NII devices, in the sense that it does not require the complete software package to be protected, but only requires that the radio cannot be operated by third parties in an unauthorized manner. If this change is adopted, rules regarding the equipment authorization process[16] do not have to be modified. The idea behind the proposed rule is that a hardware barrier limits radio parameters to authorized values only, i.e., to parameter ranges as specified in an FCC certification of the device. By supplying a small configuration file that is signed by the original manufacturer, it is possible to enable additional radio parameters. This allows the original manufacturer, possibly after going through a new FCC certification process, to unlock additional radio parameters (e.g., enabling a new channel) by specifying this in the configuration file, and then signing this file. A few remarks are in place:

1. The proposed rule does not state that all software loaded on the device must be secured. Instead, it limits itself only to radio operations. Hence this rule is within authority of the Commission to propose and adopt.
2. Third parties can modify the software with the assurance that the radio will only operate using authorized radio parameters. In other words, third parties can modify operations which are unrelated to transmission or reception of signals, but cannot influence the operation of the radio so it would operate using unauthorized radio parameters.
3. The original manufacturer can include a signed configuration file to, for example, unlock additional channels or transmit powers. Note that this does not require signing the complete software package. Instead, the signature is created only over a small configuration file. If the signature is valid, the radio (hardware) can read the configuration file and unlock the specified radio parameters. Essentially the signature proves the device has been authorized by the FCC and/or manufacturer to operate under new radio parameters. Third parties cannot modify this configuration file since that would invalidate the signature. Hence, while third parties can always

---

[16] See 47 C.F.R. §2.1033(a)(4)(i)

modify functionality unrelated to radio operations, they are unable to operate the radio in an unauthorized manner.

To conclude, since third parties cannot create valid signatures, they can't unlock additional radio parameters. Only the original manufacturer can do this. It may also be worthwhile to consider whether part of the device security rules for U-NII devices can be simplified. Point one of rule 47 C.F.R. §2.1033(b)(13)[17] is no longer needed if the proposed rule in this section will be adopted. Indeed, the proposed SDR rule in this section is actually based on the security rules for U-NII devices.

6. Conclusion

By relying on the American Library Association v. FCC ruling,[18] a strong case can be made that the proposed rules by the Commission lie outside its authority. Additionally, the security rules proposed by the Commission would directly harm researchers, and make it impossible to carry out certain research experiments. Fortunately, the proposed rules can be modified so these issues are avoided, while still assuring that third parties cannot operate the radio in an unauthorized manner.

Respectfully submitted,

Mathy Vanhoef
Doctoral Researcher in wireless security
KU Leuven, Dept. Computerwetenschappen
Celestijnenlaan 200a, bus 2402
Heverlee, 3001, Belgium

9 October 2015

---

[17] This concerns security features of U-NII devices so third parties cannot operate the device outside parameters for which the device was certified.

[18] See *American Library Association v. FCC*, 406 F.3d 689 (D.C. Cir. 2005)